

# ASYMPTOTICS OF THE NUMBER OF INVOLUTIONS IN FINITE CLASSICAL GROUPS

JASON FULMAN, ROBERT GURALNICK, AND DENNIS STANTON

**ABSTRACT.** Answering a question of Geoff Robinson, we compute the large  $n$  limiting proportion of  $i(n, q)/q^{\lfloor n^2/2 \rfloor}$ , where  $i(n, q)$  denotes the number of involutions in  $GL(n, q)$ . We give similar results for the finite unitary, symplectic, and orthogonal groups, in both odd and even characteristic. At the heart of this work are certain new “sum=product” identities. Our self-contained treatment of the enumeration of involutions in even characteristic symplectic and orthogonal groups may also be of interest.

## 1. INTRODUCTION

On math overflow, Dima Pasechnik asked about the asymptotic behavior of the number of involutions in  $GL(n, 2)$ , as  $n \rightarrow \infty$ . Again on math overflow, Geoff Robinson observed that for  $n$  even, the number of involutions in  $GL(n, 2)$  is “unreasonably close” to the estimate  $2^{n^2/2}$ . In an email to us in October 2015, Robinson asked whether for  $n$  even we could compute the limiting value of  $i(n, 2)/2^{n^2/2}$ , where  $i(n, 2)$  is the number of involutions in  $GL(n, 2)$ , and asserted that he could show that this limiting value should be between  $3/4$  and something probably larger than  $2$ .

Letting  $i(n, q)$  denote the number of involutions in  $GL(n, q)$ , we are able to compute the more general limiting proportion  $i(n, q)/q^{\lfloor n^2/2 \rfloor}$ . The answer depends on whether  $n$  is even or odd and on whether  $q$  is even or odd. For example if  $n$  is even, and if  $q$  is even and fixed, it is shown in Section 3 that

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{i(n, q)}{q^{n^2/2}} &= \frac{1}{2} \left[ \prod_{i \geq 1} (1 + \sqrt{q}/q^i) + \prod_{i \geq 1} (1 - \sqrt{q}/q^i) \right] \\ &= \prod_{i \geq 1} \frac{(1 + q^{5-8i})(1 + q^{3-8i})(1 - q^{-8i})}{(1 - q^{-2i})}. \end{aligned}$$

When  $q = 2$  this is  $1.6793\dots$ , which is indeed between  $3/4$  and something probably larger than  $2$ . The reason for dividing by  $q^{n^2/2}$  is that for  $n$  even,

---

*Date:* February 9, 2016.

*Key words and phrases.* involution, finite classical group.

*2010 AMS Subject Classification:* 05E99, 20G40.

$n^2/2$  is the dimension (in the algebraic group) of the largest conjugacy class of involutions. Similarly when  $n$  is odd, one divides by  $q^{(n^2-1)/2}$ .

At the heart of these results for  $GL(n, q)$  are the following “sum=product” identities, proved in [3]. These identities state that:

$$\sum_{n \geq 0} u^n q^{\binom{n}{2}} \sum_{r=0}^{\lfloor n/2 \rfloor} \frac{1}{q^{r(2n-3r)} |GL(r, q)| |GL(n-2r, q)|} = \frac{\prod_{i \geq 1} (1 + u/q^i)}{\prod_{i \geq 1} (1 - u^2/q^i)}.$$

$$\sum_{n \geq 0} u^n q^{\binom{n}{2}} \sum_{r=0}^n \frac{1}{|GL(r, q)| |GL(n-r, q)|} = \frac{\prod_{i \geq 1} (1 + u/q^i)^2}{\prod_{i \geq 1} (1 - u^2/q^i)}.$$

The first identity is useful for even characteristic, and the second identity is useful for odd characteristic. We give new proofs of these identities, and derive analogous identities for the other finite classical groups, which we believe to be interesting and new. For example in the case of odd characteristic symplectic groups, we show that

$$\sum_{n \geq 0} u^n q^{n^2} \sum_{r=0}^n \frac{1}{|Sp(2r, q)| |Sp(2n-2r, q)|} = \frac{\prod_{i \geq 1} (1 + u/q^{2i})^2}{\prod_{i \geq 1} (1 - u^2/q^{2i})}.$$

The proof of the even characteristic symplectic identity is tricky, as are the orthogonal group identities.

The point of these identities is that it allows us to obtain product formulae for the generating functions for proportions of involutions in finite classical groups. These product formulae are perfectly suited for asymptotic analysis, using the following elementary lemma of Darboux (given an exposition in [6]).

**Lemma 1.1.** *Suppose that  $f(u)$  is analytic for  $|u| < r, r > 0$  and has a finite number of simple poles on  $|u| = r$ . Let  $w_j$  denote the poles, and suppose that  $f(u) = \sum_j \frac{g_j(u)}{1-u/w_j}$  with  $g_j(u)$  analytic near  $w_j$ . Then the coefficient of  $u^n$  in  $f(u)$  is*

$$\sum_j \frac{g_j(w_j)}{w_j^n} + o(1/r^n).$$

For each of the families of groups we consider, we get an infinite product formula for the limiting value of  $i(n, q)/q^{d(n, q)}$  for  $q$  fixed and  $n \rightarrow \infty$ . Here  $d(n, q)$  is the dimension of the variety of involutions in the corresponding algebraic group. It turns out that the limit of this formula as  $q \rightarrow \infty$  is precisely the number of components of maximal dimension in the variety (in every case this is either 1 or 2).

This paper is organized as follows. Section 2 derives many “sum=product” identities which are crucial to our work. The remaining sections study asymptotics of the number of involutions. Section 3 treats the general linear groups. Section 4 treats the unitary groups. Section 5 treats the

symplectic groups, and Section 6 treats the orthogonal groups. We mention that Sections 5 and 6 give self-contained derivations of the number of involutions in the symplectic and orthogonal groups. While this is easy in odd characteristic, the enumeration of involutions in even characteristic is subtle (see [2], [4] for related results).

To close the introduction, we make three remarks about future work. First, it would be interesting to find proofs of our results which do not require generating functions. Second, our methods will work for the subgroups  $SO$  and  $\Omega$  of the orthogonal groups. Third, enumeration of involutions is connected to representation theory via Frobenius-Schur indicators. This is developed for  $GL$  and  $U$  in [3], but much remains to be done for other finite classical groups.

## 2. IDENTITIES

This section derives some “sum=product” identities which will be crucially applied later in the paper.

Throughout this section (and the rest of this paper) we use the following notation:

$$(A; q)_n = \prod_{k=0}^{n-1} (1 - Aq^k), \quad (A; q)_\infty = \prod_{k=0}^{\infty} (1 - Aq^k) \text{ if } -1 < q < 1.$$

Theorem 2.1 (the  $q$ -binomial theorem) will be used throughout. See page 17 of [1] for a proof.

**Theorem 2.1.** *If  $-1 < q < 1$  and  $|x| < 1$ , then*

$$\sum_{n=0}^{\infty} \frac{(A; q)_n}{(q; q)_n} x^n = \frac{(Ax; q)_\infty}{(x; q)_\infty}.$$

The following two well known special cases are used.

**Corollary 2.2.** *If  $-1 < q < 1$  and  $|x| < 1$ , then*

$$\sum_{n=0}^{\infty} \frac{x^n}{(q; q)_n} = \frac{1}{(x; q)_\infty}.$$

*Proof.* Set  $A = 0$  in Theorem 2.1. □

**Corollary 2.3.** *If  $-1 < q < 1$ , then*

$$\sum_{n=0}^{\infty} \frac{x^n q^{\binom{n}{2}}}{(q; q)_n} = (-x; q)_\infty.$$

*Proof.* Replace  $x$  by  $-x/A$  in Theorem 2.1, and let  $A \rightarrow \infty$ . □

Lemma 2.4 is one of our main lemmas.

**Lemma 2.4.** *If  $1 < |q|$ , and  $|ab/q| < 1$ , then*

$$\begin{aligned} \sum_{m=0}^{\infty} q^{\binom{m}{2}} \sum_{k=0}^m \frac{(-a)^{m-k} (-b)^k}{(q; q)_k q^{\binom{k}{2}} (q; q)_{m-k} q^{\binom{m-k}{2}}} \\ = \frac{(-a/q; 1/q)_{\infty} (-b/q; 1/q)_{\infty}}{(ab/q; 1/q)_{\infty}} = H(a, b, q). \end{aligned}$$

*Proof.* Let  $Q = 1/q$ . Replacing  $m$  by  $m+k$ , the double sum is

$$D = \sum_{k=0}^{\infty} \sum_{m=0}^{\infty} \frac{a^m b^k}{(Q; Q)_k (Q; Q)_m} Q^{\binom{k+1}{2} + \binom{m+1}{2} - mk}.$$

The  $m$ -sum is evaluable by Corollary 2.3 to

$$\begin{aligned} (-aQ^{1-k}; Q)_{\infty} &= (-aQ^{1-k}; Q)_k (-aQ; Q)_{\infty} \\ &= (-1/a; Q)_k (-aQ; Q)_{\infty} a^k Q^{-\binom{k}{2}}. \end{aligned}$$

So

$$D = (-aQ; Q)_{\infty} \sum_{k=0}^{\infty} \frac{(-1/a; Q)_k}{(Q; Q)_k} (abQ)^k = \frac{(-aQ; Q)_{\infty} (-bQ; Q)_{\infty}}{(abQ; Q)_{\infty}}$$

by Theorem 2.1. □

There is a companion lemma which is also useful.

**Lemma 2.5.** *If  $1 < |q|$ ,  $s$  and  $t$  are non-negative integers, and  $|bq^{-s/2}| < 1$ , then*

$$\begin{aligned} \sum_{n=0}^{\infty} q^{\binom{n}{2}} \sum_{r=0}^{\lfloor (n-t)/s \rfloor} \frac{a^{n-sr} b^r}{q^{r^2} (1/q; 1/q)_r q^{(n-sr-t)^2} (1/q; 1/q)_{n-rs-t} q^{r(sn-(1+s^2/2)r)}} \\ = a^t q^{\binom{t}{2}} \frac{(-aq^{t-1}; 1/q)_{\infty}}{(bq^{-s/2}; 1/q)_{\infty}} = G(a, b, q, s, t). \end{aligned}$$

*Proof.* Replacing  $n$  by  $n+rs+t$  one obtains

$$G(a, b, q, s, t) = a^t q^{\binom{t}{2}} \sum_{r=0}^{\infty} \frac{(bq^{-s/2})^r}{(1/q; 1/q)_r} \sum_{n=0}^{\infty} \frac{q^{-\binom{n}{2}} (aq^{t-1})^n}{(1/q; 1/q)_n}.$$

Then apply Corollaries 2.2 and 2.3. □

Proposition 2.6 will be useful for writing certain sums and differences of infinite products as a single infinite product. It will also be crucial for treating the unitary groups.

**Proposition 2.6.** *Let  $-1 < R < 1$  and*

$$F(X, R) = (R; R)_{\infty} (-X; R)_{\infty} (-R/X; R)_{\infty}.$$

Then

$$\begin{aligned}\frac{1}{2}(F(X, R) + F(-X, R)) &= F(RX^2, R^4), \\ \frac{1}{2}(F(X, R) - F(-X, R)) &= XF(R^3X^2, R^4).\end{aligned}$$

*Proof.* Use the Jacobi triple product identity ([1], p.21)

$$F(X, R) = \sum_{n=-\infty}^{\infty} R^{\binom{n}{2}} X^n$$

to find the even and odd parts of  $F(X, R)$ .  $\square$

Theorem 2.7 will be useful in treating even characteristic general linear and unitary groups. Recall that in any characteristic,  $|GL(j, q)| = q^{\binom{j}{2}}(q^j - 1) \cdots (q - 1)$ . Theorem 2.7 appeared as Corollary 3.5 of [3], but for completeness we give a different proof here.

**Theorem 2.7.** *For  $q > 1$  and  $u^2 < q$ ,*

$$\sum_{n \geq 0} u^n q^{\binom{n}{2}} \sum_{r=0}^{\lfloor n/2 \rfloor} \frac{1}{q^{r(2n-3r)} |GL(r, q)| |GL(n-2r, q)|} = \frac{\prod_{i \geq 1} (1 + u/q^i)}{\prod_{i \geq 1} (1 - u^2/q^i)}.$$

*Proof.* Because

$$(1) \quad |GL(r, q)| = q^{r^2} (1/q; 1/q)_r,$$

we use Lemma 2.5 to evaluate the double sum, which is  $G(u, u^2, q, 2, 0)$ .  $\square$

Theorem 2.8 will be helpful in treating odd characteristic general linear and unitary groups. This result was Corollary 3.7 of [3], but we give a different (and simpler) proof here.

**Theorem 2.8.** *For  $q > 1$  and  $u^2 < q$ ,*

$$\sum_{n \geq 0} u^n q^{\binom{n}{2}} \sum_{r=0}^n \frac{1}{|GL(r, q)| |GL(n-r, q)|} = \frac{\prod_{i \geq 1} (1 + u/q^i)^2}{\prod_{i \geq 1} (1 - u^2/q^i)}.$$

*Proof.* Using (1), we can apply Lemma 2.4 to evaluate the double sum, which is  $H(u, u, q)$ .  $\square$

The next four theorems will be useful in our analysis of the unitary groups.

**Theorem 2.9.** *Let  $i = \sqrt{-1}$ . Then for  $q > 1$ ,*

$$\begin{aligned}& \frac{1}{2} \left[ \prod_{j \geq 1} (1 + i\sqrt{q}/(-q)^j) + \prod_{j \geq 1} (1 - i\sqrt{q}/(-q)^j) \right] \\ &= \prod_{k \geq 1} \frac{(1 - q^{3-8k})(1 - q^{5-8k})(1 - q^{-8k})}{(1 - q^{-2k})}.\end{aligned}$$

*Proof.* Let  $Q = -1/q$ . Note that if  $X = iQ\sqrt{-1/Q} = -i\sqrt{-Q}$ , we have  $QX^2 = Q^2$ . Thus letting  $F$  be as in Proposition 2.6,

$$\begin{aligned}
& \frac{1}{2} \left[ \prod_{j \geq 1} (1 + i\sqrt{-1/Q}Q^j) + \prod_{j \geq 1} (1 - i\sqrt{-1/Q}Q^j) \right] \\
&= \frac{1}{2} ((-X; Q^2)_\infty (-QX; Q^2)_\infty + (X; Q^2)_\infty (QX; Q^2)_\infty) \\
&= \frac{1}{2} \frac{1}{(Q^2; Q^2)_\infty} (F(X, Q^2) + F(-X, Q^2)) \\
&= \frac{1}{(Q^2; Q^2)_\infty} F(Q^3, Q^8).
\end{aligned}$$

In the last step we have applied Proposition 2.6 with  $R = Q^2$ .  $\square$

**Theorem 2.10.** *Let  $i = \sqrt{-1}$ . Then for  $q > 1$ ,*

$$\begin{aligned}
& \frac{i}{2} \left[ \prod_{j \geq 1} (1 + i\sqrt{q}/(-q)^j) - \prod_{j \geq 1} (1 - i\sqrt{q}/(-q)^j) \right] \\
&= \frac{1}{\sqrt{q}} \prod_{k \geq 1} \frac{(1 - q^{1-8k})(1 - q^{7-8k})(1 - q^{-8k})}{(1 - q^{-2k})}.
\end{aligned}$$

*Proof.* Let  $Q = -1/q$ . Note that if  $X = iQ\sqrt{-1/Q} = -i\sqrt{-Q}$ , we have  $QX^2 = Q^2$ . Thus

$$\begin{aligned}
& \frac{i}{2} \left[ \prod_{j \geq 1} (1 + i\sqrt{-1/Q}Q^j) - \prod_{j \geq 1} (1 - i\sqrt{-1/Q}Q^j) \right] \\
&= \frac{i}{2} ((-X; Q^2)_\infty (-QX; Q^2)_\infty - (X; Q^2)_\infty (QX; Q^2)_\infty) \\
&= \frac{i}{2} \frac{1}{(Q^2; Q^2)_\infty} (F(X, Q^2) - F(-X, Q^2)) \\
&= \frac{\sqrt{-Q}}{(Q^2; Q^2)_\infty} F(Q^7, Q^8).
\end{aligned}$$

In the last step we have applied Proposition 2.6 with  $R = Q^2$ .  $\square$

**Theorem 2.11.** *Let  $i = \sqrt{-1}$ . Then for  $q > 1$ ,*

$$\begin{aligned}
& \frac{1}{2} \left[ \prod_{j \geq 1} (1 + i\sqrt{q}/(-q)^j)^2 + \prod_{j \geq 1} (1 - i\sqrt{q}/(-q)^j)^2 \right] \\
&= \prod_{k \geq 1} \frac{(1 + q^{2-4k})^2(1 - q^{-4k})}{(1 - (-1/q)^k)}.
\end{aligned}$$

*Proof.* Let  $Q = -1/q$ . Note that if  $X = iQ\sqrt{-1/Q} = -i\sqrt{-Q}$ , we have  $X^2 = Q$ . Thus

$$\begin{aligned} & \frac{1}{2} \left[ \prod_{j \geq 1} (1 + i\sqrt{-1/Q}Q^j)^2 + \prod_{j \geq 1} (1 - i\sqrt{-1/Q}Q^j)^2 \right] \\ &= \frac{1}{2} ((-X; Q)_\infty (-Q/X; Q)_\infty + (X; Q)_\infty (Q/X; Q)_\infty) \\ &= \frac{1}{2} \frac{1}{(Q; Q)_\infty} (F(X, Q) + F(-X, Q)) \\ &= \frac{1}{(Q; Q)_\infty} F(Q^2, Q^4), \end{aligned}$$

where we have applied Proposition 2.6 with  $R = Q$ .  $\square$

**Theorem 2.12.** *Let  $i = \sqrt{-1}$ . Then for  $q > 1$ ,*

$$\begin{aligned} & \frac{i}{2} \left[ \prod_{j \geq 1} (1 + i\sqrt{q}/(-q)^j)^2 - \prod_{j \geq 1} (1 - i\sqrt{q}/(-q)^j)^2 \right] \\ &= \frac{2}{\sqrt{q}} \prod_{k \geq 1} \frac{(1 + q^{-4k})^2 (1 - q^{-4k})}{(1 - (-1/q)^k)}. \end{aligned}$$

*Proof.* Let  $Q = -1/q$ . Note that if  $X = iQ\sqrt{-1/Q} = -i\sqrt{-Q}$ , we have  $X^2 = Q$ . Thus

$$\begin{aligned} & \frac{i}{2} \left[ \prod_{j \geq 1} (1 + i\sqrt{-1/Q}Q^j)^2 - \prod_{j \geq 1} (1 - i\sqrt{-1/Q}Q^j)^2 \right] \\ &= \frac{i}{2} ((-X; Q)_\infty (-Q/X; Q)_\infty - (X; Q)_\infty (Q/X; Q)_\infty) \\ &= \frac{i}{2} \frac{1}{(Q; Q)_\infty} (F(X, Q) - F(-X, Q)) \\ &= \frac{\sqrt{-Q}}{(Q; Q)_\infty} F(Q^4, Q^4). \end{aligned}$$

where we have applied Proposition 2.6 with  $R = Q$ .  $\square$

Theorem 2.13 gives a useful “sum=product” formula for the symplectic groups in odd characteristic. Recall that in any characteristic,

$$(2) \quad |Sp(2n, q)| = q^{n^2} \prod_{i=1}^n (q^{2i} - 1) = q^{2n^2+n} (1/q^2; 1/q^2)_n.$$

**Theorem 2.13.** *For  $q > 1$  and  $|u| < q$ ,*

$$\sum_{n \geq 0} u^n q^{n^2} \sum_{r=0}^n \frac{1}{|Sp(2r, q)| |Sp(2n-2r, q)|} = \frac{\prod_{i \geq 1} (1 + u/q^{2i})^2}{\prod_{i \geq 1} (1 - u^2/q^{2i})}.$$

*Proof.* We can apply (2) and Lemma 2.4 to evaluate the double sum, which is  $H(u, u, q^2)$ .  $\square$

The following rather tricky identity will be useful for treating even characteristic symplectic groups.

**Theorem 2.14.** *For  $q > 1$  and  $|u| < 1$ ,*

$$\sum_{n \geq 0} u^n q^{n^2} \left( \sum_{\substack{r=0 \\ r \text{ even}}}^n \frac{1}{A_r} + \sum_{\substack{r=1 \\ r \text{ even}}}^n \frac{1}{B_r} + \sum_{\substack{r=1 \\ r \text{ odd}}}^n \frac{1}{C_r} \right) = \frac{1}{1-u} \frac{\prod_{i \geq 1} (1 + u/q^{2i})}{\prod_{i \geq 1} (1 - u^2/q^{2i})}.$$

where

$$\begin{aligned} A_r &= q^{r(r+1)/2 + r(2n-2r)} |Sp(r, q)| |Sp(2n-2r, q)|, \\ B_r &= q^{r(r+1)/2 + r(2n-2r)} q^{r-1} |Sp(r-2, q)| |Sp(2n-2r, q)|, \\ C_r &= q^{r(r+1)/2 + r(2n-2r)} |Sp(r-1, q)| |Sp(2n-2r, q)|. \end{aligned}$$

*Proof.* Each of the three double sums may be computed using Lemma 2.5.

Replacing  $r$  by  $2r$ ,  $2r+2$ , and  $2r+1$  respectively in these three double sums, we see that the three sums become

$$\begin{aligned} & G(u, u^2, q^2, 2, 0) + q^6 G(u/q^4, u^2 q^2, q^2, 2, 2) + q^2 G(u/q^2, u^2 q^2, q^2, 2, 1) \\ &= (-u/q^2; 1/q^2)_\infty \left( \frac{1}{(u^2/q^2; 1/q^2)_\infty} + \frac{u^2}{(u^2; 1/q^2)_\infty} + \frac{u}{(u^2; 1/q^2)_\infty} \right) \\ &= \frac{1}{1-u} \frac{(-u/q^2; 1/q^2)_\infty}{(u^2/q^2; 1/q^2)_\infty} \end{aligned}$$

$\square$

Next we prove three “sum=product” identities which will be useful for studying odd characteristic orthogonal groups. Recall that in any characteristic,

(3)

$$|O^+(2n+1, q)| = |O^-(2n+1, q)| = 2q^{n^2} \prod_{i=1}^n (q^{2i} - 1) = 2q^{2n^2+n} (1/q^2; 1/q^2)_n.$$

and that  $|O^+(1, q)| = |O^-(1, q)| = 2$ . Recall also that in any characteristic, for  $n \geq 1$ ,

$$(4) \quad |O^\pm(2n, q)| = \frac{2q^{n^2-n}}{q^n \pm 1} \prod_{i=1}^n (q^{2i} - 1) = \frac{2q^{2n^2}}{q^n \pm 1} (1/q^2; 1/q^2)_n.$$

and that  $|O^+(0, q)| = 1$ .

Our first identity is useful in treating odd characteristic even dimensional orthogonal groups of positive type.



**Theorem 2.15.** For  $q > 1$  and  $|u| < 1/q$ ,

$$\begin{aligned} & \sum_{n \geq 0} u^n q^{n^2} \\ & \cdot \left[ \sum_{r=0}^{2n} \frac{1}{|O^+(r, q)| |O^+(2n-r, q)|} + \sum_{r=1}^{2n-1} \frac{1}{|O^-(r, q)| |O^-(2n-r, q)|} \right] \\ & = \frac{1}{2(1-ug)} \frac{\prod_{i \geq 1} (1 + u/q^{2(i-1)})^2}{\prod_{i \geq 1} (1 - u^2/q^{2(i-1)})} + \frac{1}{2} \frac{\prod_{i \geq 1} (1 + u/q^{2i-1})^2}{\prod_{i \geq 1} (1 - u^2/q^{2(i-1)})}. \end{aligned}$$

*Proof.* It suffices to show that the left-hand side of the statement of Theorem 2.15 is equal to

$$\frac{1}{2} \left[ \frac{(-u/q; 1/q^2)_\infty^2}{(u^2; 1/q^2)_\infty} + (1+ug) \frac{(-u; 1/q^2)_\infty^2}{(q^2 u^2; 1/q^2)_\infty} \right].$$

Because the value of  $|O^+(r, q)|$  depends on the parity of  $r$ , we split each sum into two sums, depending on the parity of  $r$ .

CASE 1:  $r = 2R$ , first sum:

$$S_1 = \frac{1}{4} \sum_{n=0}^{\infty} (-u)^n q^{n^2} \sum_{R=0}^n \frac{(1+q^R)(1+q^{n-R})}{q^{R^2-R}(q^2; q^2)_R q^{(n-R)^2-(n-R)}(q^2; q^2)_{n-R}}$$

To write this in the form of Lemma 2.4 with  $q$  replaced by  $q^2$ , note that

$$q^{R^2-R} = q^{2\binom{R}{2}}, \quad q^{(n-R)^2-(n-R)} = q^{2\binom{n-R}{2}}$$

$$q^{n^2}(1+q^R)(1+q^{n-R}) = q^{2\binom{n}{2}} q^n (1+q^R)(1+q^{n-R})$$

The numerator has 4 terms  $q^n, q^{n+R}, q^{2n-R}, q^{2n}$ . We pick  $(a, b)$  in Lemma 2.4, so that these four terms appear. The choices are  $(a, b) = (uq, uq)$ ,  $(a, b) = (uq, uq^2)$ ,  $(a, b) = (uq^2, uq)$ , and  $(a, b) = (uq^2, uq^2)$  respectively to obtain

$$S_1 = \frac{1}{4} \left[ \frac{(-u/q; 1/q^2)_\infty^2}{(u^2; 1/q^2)_\infty} + 2 \frac{(-u/q; 1/q^2)_\infty (-u; 1/q^2)_\infty}{(qu^2; 1/q^2)_\infty} + \frac{(-u; 1/q^2)_\infty^2}{(q^2 u^2; 1/q^2)_\infty} \right]$$

CASE 2:  $r = 2R + 1$ , first sum:

$$S_2 = \frac{1}{4} \sum_{n=1}^{\infty} u^n q^{n^2} \sum_{R=0}^{n-1} \frac{(-1)^R (-1)^{n-1-R}}{q^{R^2}(q^2; q^2)_R q^{(n-R-1)^2}(q^2; q^2)_{n-R-1}}$$

We use Lemma 2.4 with  $q$  replaced by  $q^2$  and  $(a, b) = (uq^2, uq^2)$ ,

$$S_2 = \frac{uq}{4} \frac{(-u; 1/q^2)_\infty^2}{(u^2 q^2; 1/q^2)_\infty}.$$

CASE 3:  $r = 2R$ , second sum:

$$S_1 = \frac{1}{4} \sum_{n=0}^{\infty} (-u)^n q^{n^2} \sum_{R=0}^n \frac{(q^R - 1)(q^{n-R} - 1)}{q^{R^2-R}(q^2; q^2)_R q^{(n-R)^2-(n-R)}(q^2; q^2)_{n-R}}$$

The numerator has 4 terms  $q^n, -q^{n+R}, -q^{2n-R}, q^{2n}$ . As in CASE 1 we obtain

$$S_3 = \frac{1}{4} \left[ \frac{(-u/q; 1/q^2)_\infty^2}{(u^2; 1/q^2)_\infty} - 2 \frac{(-u/q; 1/q^2)_\infty (-u; 1/q^2)_\infty}{(qu^2; 1/q^2)_\infty} + \frac{(-u; 1/q^2)_\infty^2}{(q^2u^2; 1/q^2)_\infty} \right]$$

CASE 4:  $r = 2R + 1$ , second sum:

$$S_4 = \frac{1}{4} \sum_{n=1}^{\infty} u^n q^{n^2} \sum_{R=0}^{n-1} \frac{(-1)^R (-1)^{n-1-R}}{q^{R^2} (q^2; q^2)_R q^{(n-R-1)^2} (q^2; q^2)_{n-R-1}}$$

This is the same as CASE 2,

$$S_4 = \frac{uq}{4} \frac{(-u; 1/q^2)_\infty^2}{(u^2q^2; 1/q^2)_\infty}.$$

So

$$S_1 + S_2 + S_3 + S_4 = \frac{1}{2} \left[ \frac{(-u/q; 1/q^2)_\infty^2}{(u^2; 1/q^2)_\infty} + (1 + uq) \frac{(-u; 1/q^2)_\infty^2}{(q^2u^2; 1/q^2)_\infty} \right]$$

□

Our second identity is useful in treating odd characteristic even dimensional orthogonal groups of negative type.

**Theorem 2.16.** *For  $q > 1$  and  $|u| < 1/q$ ,*

$$\begin{aligned} & \sum_{n \geq 0} u^n q^{n^2} \\ & \cdot \left[ \sum_{r=0}^{2n-1} \frac{1}{|O^+(r, q)| |O^-(2n-r, q)|} + \sum_{r=1}^{2n} \frac{1}{|O^-(r, q)| |O^+(2n-r, q)|} \right] \\ & = \frac{1}{2(1-uq)} \frac{\prod_{i \geq 1} (1 + u/q^{2(i-1)})^2}{\prod_{i \geq 1} (1 - u^2/q^{2(i-1)})} - \frac{1}{2} \frac{\prod_{i \geq 1} (1 + u/q^{2i-1})^2}{\prod_{i \geq 1} (1 - u^2/q^{2(i-1)})}. \end{aligned}$$

*Proof.* It suffices to prove that the left hand side of Theorem 2.16 is equal to

$$\frac{1}{2} \left[ -\frac{(-u/q; 1/q^2)_\infty^2}{(u^2; 1/q^2)_\infty} + (1 + uq) \frac{(-u; 1/q^2)_\infty^2}{(u^2q^2; 1/q^2)_\infty} \right].$$

Note that the two sums on the left hand side of the theorem are equal, so we focus on the first sum. Because the value of  $|O^+(r, q)|$  depends on the parity of  $r$ , we split the first sum into two cases, depending on the parity of  $r$ .

CASE 1:  $r = 2R$ :

$$S_1 = \frac{1}{4} \sum_{n=0}^{\infty} (-u)^n q^{n^2} \sum_{R=0}^n \frac{(1 + q^R)(q^{n-R} - 1)}{q^{R^2-R} (q^2; q^2)_R q^{(n-R)^2 - (n-R)} (q^2; q^2)_{n-R}}$$

The numerator has 4 terms  $-q^n, -q^{n+R}, q^{2n-R}, q^{2n}$ . The middle two terms cancel, so as in CASE 1 of Theorem 2.15

$$S_1 = \frac{1}{4} \left[ -\frac{(-u/q; 1/q^2)_\infty^2}{(u^2; 1/q^2)_\infty} + \frac{(-u; 1/q^2)_\infty^2}{(q^2 u^2; 1/q^2)_\infty} \right]$$

CASE 2:  $r = 2R + 1$ : As in CASE 2 of Theorem 2.15

$$\begin{aligned} S_2 &= \frac{1}{4} \sum_{n=1}^{\infty} u^n q^{n^2} \sum_{R=0}^{n-1} \frac{(-1)^R (-1)^{n-1-R}}{q^{R^2} (q^2; q^2)_R q^{(n-R-1)^2} (q^2; q^2)_{n-R-1}} \\ &= \frac{uq}{4} \frac{(-u; 1/q^2)_\infty^2}{(u^2 q^2; 1/q^2)_\infty} \end{aligned}$$

So we have

$$2(S_1 + S_2) = \frac{1}{2} \left[ -\frac{(-u/q; 1/q^2)_\infty^2}{(u^2; 1/q^2)_\infty} + (1 + uq) \frac{(-u; 1/q^2)_\infty^2}{(u^2 q^2; 1/q^2)_\infty} \right]$$

□

The following “sum=product” formula will be helpful in treating odd dimensional orthogonal groups in odd characteristic.

**Theorem 2.17.** For  $q > 1$  and  $|u| < 1$ ,

$$\sum_{n \geq 0} u^n q^{n^2} \cdot \left[ \sum_{r=0}^{2n+1} \frac{1}{|O^+(r, q)| |O^+(2n+1-r, q)|} + \sum_{r=1}^{2n} \frac{1}{|O^-(r, q)| |O^-(2n+1-r, q)|} \right]$$

is equal to

$$\frac{1}{1-u} \frac{\prod_{i \geq 1} (1 + u/q^{2i})^2}{\prod_{i \geq 1} (1 - u^2/q^{2i})}.$$

*Proof.* It suffices to prove that the left hand side is equal to

$$\frac{(-u; 1/q^2)_\infty (-u/q^2; 1/q^2)_\infty}{(u^2; 1/q^2)_\infty}.$$

We split each sum into two sums, depending on the parity of  $r$ .

CASE 1:  $r = 2R$ , first sum:

$$S_1 = \frac{1}{4} \sum_{n=0}^{\infty} (-u)^n q^{n^2} \sum_{R=0}^n \frac{q^{-(n-R)} (1 + q^R)}{q^{R^2-R} (q^2; q^2)_R q^{(n-R)^2 - (n-R)} (q^2; q^2)_{n-R}}$$

This is nearly CASE 1 of Theorem 2.15, the numerator has 2 terms  $q^{R-n}$  and  $q^{2R-n}$ . We apply Lemma 2.4 with  $(a, b) = (u, uq)$ ,  $(a, b) = (u, uq^2)$ , and  $q$  replaced by  $q^2$  to obtain

$$S_1 = \frac{1}{4} \left[ \frac{(-u/q^2; 1/q^2)_\infty (-u/q; 1/q^2)_\infty}{(u^2/q; 1/q^2)_\infty} + \frac{(-u/q^2; 1/q^2)_\infty (-u; 1/q^2)_\infty}{(u^2; 1/q^2)_\infty} \right]$$

CASE 2:  $r = 2R + 1$ , first sum:

$$\begin{aligned} S_2 &= \frac{1}{4} \sum_{n=0}^{\infty} (-u)^n q^{n^2} \sum_{R=0}^n \frac{(1 + q^{n-R})}{q^{R^2}(q^2; q^2)_R q^{(n-R)^2 - (n-R)}(q^2; q^2)_{n-R}} \\ &= \frac{1}{4} \left[ \frac{(-u; 1/q^2)_{\infty} (-u/q^2; 1/q^2)_{\infty}}{(u^2; 1/q^2)_{\infty}} + \frac{(-u/q; 1/q^2)_{\infty} (-u/q^2; 1/q^2)_{\infty}}{(u^2/q; 1/q^2)_{\infty}} \right]. \end{aligned}$$

where we used Lemma 2.4 with  $(a, b) = (uq^2, u)$ ,  $(a, b) = (uq, u)$  and  $q$  replaced by  $q^2$ .

CASE 3:  $r = 2R$ , second sum:

$$S_3 = \frac{1}{4} \sum_{n=0}^{\infty} (-u)^n q^{n^2} \sum_{R=0}^n \frac{(q^R - 1)}{q^{R^2-R}(q^2; q^2)_R q^{(n-R)^2}(q^2; q^2)_{n-R}}$$

The numerator has 2 terms  $q^n q^{-(n-R)}(q^R - 1) = q^{2R} - q^R$ . Using  $(a, b) = (u, uq^2)$ ,  $(a, b) = (u, uq)$  and  $q$  replaced by  $q^2$  in Lemma 2.4, we obtain

$$S_3 = \frac{1}{4} \left[ \frac{(-u/q^2; 1/q^2)_{\infty} (-u; 1/q^2)_{\infty}}{(u^2; 1/q^2)_{\infty}} - \frac{(-u/q^2; 1/q^2)_{\infty} (-u/q; 1/q^2)_{\infty}}{(u^2/q; 1/q^2)_{\infty}} \right]$$

CASE 4:  $r = 2R + 1$ , second sum:

$$S_4 = \frac{1}{4} \sum_{n=0}^{\infty} (-u)^n q^{n^2} \sum_{R=0}^n \frac{(q^{n-R} - 1)}{q^{R^2}(q^2; q^2)_R q^{(n-R)^2 - (n-R)}(q^2; q^2)_{n-R}}$$

This is basically the same as CASE 2,

$$S_4 = \frac{1}{4} \left[ \frac{(-u; 1/q^2)_{\infty} (-u/q^2; 1/q^2)_{\infty}}{(u^2; 1/q^2)_{\infty}} - \frac{(-u/q; 1/q^2)_{\infty} (-u/q^2; 1/q^2)_{\infty}}{(u^2/q; 1/q^2)_{\infty}} \right].$$

So we have

$$S_1 + S_2 + S_3 + S_4 = \frac{(-u; 1/q^2)_{\infty} (-u/q^2; 1/q^2)_{\infty}}{(u^2; 1/q^2)_{\infty}}.$$

□

Finally, we give two identities which will be useful for analyzing the number of involutions in even characteristic orthogonal groups.

Theorem 2.18 will be useful for positive type orthogonal groups in even characteristic.

**Theorem 2.18.** *For  $q > 1$  and  $|u| < 1/q$ ,*

$$\begin{aligned} & \sum_{n \geq 0} q^{n^2} u^n \left[ \sum_{\substack{r=0 \\ r \text{ even}}}^n \frac{1}{A_r} + \sum_{\substack{r=1 \\ r \text{ even}}}^n \frac{1}{B_r} + \sum_{\substack{r=1 \\ r \text{ odd}}}^n \frac{1}{C_r} \right] \\ &= \frac{1}{2(1-uv)} \frac{\prod_{i \geq 1} (1 + u/q^{2(i-1)})}{\prod_{i \geq 1} (1 - u^2/q^{2(i-1)})} + \frac{1}{2} \frac{\prod_{i \geq 1} (1 + u/q^{2i-1})}{\prod_{i \geq 1} (1 - u^2/q^{2(i-1)})}, \end{aligned}$$

where

$$A_r = q^{r(r-1)/2+r(2n-2r)} |Sp(r, q)| |O^+(2n-2r, q)|$$

$$B_r = 2q^{r(r+1)/2+(r-1)(2n-2r)-1} |Sp(r-2, q)| |Sp(2n-2r, q)|$$

$$C_r = 2q^{r(r-1)/2+(r-1)(2n-2r)} |Sp(r-1, q)| |Sp(2n-2r, q)|.$$

*Proof.* The first double sum, after replacing  $r$  by  $2r$ , may be rewritten, after using (2), (4), and Lemma 2.5, as

$$\frac{1}{2} (G(uq^2, u^2q^2, q^2, 2, 0) + G(uq, u^2q^2, q^2, 2, 0)).$$

The last two double sums, after replacing  $r$  by  $2r+2$  and  $2r+1$  respectively, are

$$\frac{1}{2} (q^4 G(u/q^2, u^2q^4, q^2, 2, 2) + q^1 G(u, u^2q^4, q^2, 2, 1)).$$

The identity

$$\begin{aligned} & \frac{1}{2} (G(uq^2, u^2q^2, q^2, 2, 0) + q^4 G(u/q^2, u^2q^4, q^2, 2, 2) + q^1 G(u, u^2q^4, q^2, 2, 1)) \\ &= \frac{1}{2(1-ug)} \frac{(-u; 1/q^2)_\infty}{(u^2; 1/q^2)_\infty} \end{aligned}$$

completes the proof.  $\square$

Theorem 2.19 will be useful for negative type orthogonal groups in even characteristic.

**Theorem 2.19.** For  $q > 1$  and  $|u| < 1/q$ ,

$$\begin{aligned} & \sum_{n \geq 0} q^{n^2} u^n \left[ \sum_{\substack{r=0 \\ r \text{ even}}}^{n-1} \frac{1}{A_r} + \sum_{\substack{r=1 \\ r \text{ even}}}^n \frac{1}{B_r} + \sum_{\substack{r=1 \\ r \text{ odd}}}^n \frac{1}{C_r} \right] \\ &= \frac{1}{2(1-ug)} \frac{\prod_{i \geq 1} (1 + u/q^{2(i-1)})}{\prod_{i \geq 1} (1 - u^2/q^{2(i-1)})} - \frac{1}{2} \frac{\prod_{i \geq 1} (1 + u/q^{2i-1})}{\prod_{i \geq 1} (1 - u^2/q^{2(i-1)})}, \end{aligned}$$

where

$$A_r = q^{r(r-1)/2+r(2n-2r)} |Sp(r, q)| |O^-(2n-2r, q)|$$

$$B_r = 2q^{r(r+1)/2+(r-1)(2n-2r)-1} |Sp(r-2, q)| |Sp(2n-2r, q)|$$

$$C_r = 2q^{r(r-1)/2+(r-1)(2n-2r)} |Sp(r-1, q)| |Sp(2n-2r, q)|.$$

*Proof.* The only change to the proof of Theorem 2.18, is that the first double sum has a minus sign in the numerator factor for  $|O^-(2n-2r, q)|$ . The term  $r = n$  may be allowed because the last part of (4) has  $1/|O^-(0, q)| = 0$ .  $\square$

## 3. GENERAL LINEAR GROUPS

This section studies asymptotics of the number of involutions in  $GL(n, q)$ , when  $q$  is fixed and  $n \rightarrow \infty$ . Throughout we let  $i(n, q)$  denote the number of involutions in  $GL(n, q)$ . The following explicit formula for  $i(n, q)$  can be found in Section 1.11 of [5].

**Proposition 3.1.** *The number of involutions in  $GL(n, q)$  is*

$$i(n, q) = \begin{cases} \sum_{r=0}^{\lfloor n/2 \rfloor} \frac{|GL(n, q)|}{q^{r(2n-3r)} |GL(r, q)| |GL(n-2r, q)|}, & \text{for } q \text{ even,} \\ \sum_{r=0}^n \frac{|GL(n, q)|}{|GL(r, q)| |GL(n-r, q)|}, & \text{for } q \text{ odd.} \end{cases}$$

To begin we treat the case of even characteristic.

**Theorem 3.2.** (1) *Let  $n$  be even and let  $q$  be even and fixed. Then*

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{i(n, q)}{q^{n^2/2}} &= \frac{1}{2} \left[ \prod_{i \geq 1} (1 + \sqrt{q}/q^i) + \prod_{i \geq 1} (1 - \sqrt{q}/q^i) \right] \\ &= \prod_{i \geq 1} \frac{(1 + q^{5-8i})(1 + q^{3-8i})(1 - q^{-8i})}{(1 - q^{-2i})}. \end{aligned}$$

(2) *Let  $n$  be odd and let  $q$  be even and fixed. Then*

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{i(n, q)}{q^{(n^2-1)/2}} &= \frac{\sqrt{q}}{2} \left[ \prod_{i \geq 1} (1 + \sqrt{q}/q^i) - \prod_{i \geq 1} (1 - \sqrt{q}/q^i) \right] \\ &= \prod_{i \geq 1} \frac{(1 + q^{7-8i})(1 + q^{1-8i})(1 - q^{-8i})}{(1 - q^{-2i})}. \end{aligned}$$

*Proof.* Replacing  $u$  by  $u\sqrt{q}$  in Theorem 2.7 gives that

$$(5) \quad \sum_{n \geq 0} u^n q^{n/2} q^{\binom{n}{2}} \sum_{r=0}^{\lfloor n/2 \rfloor} \frac{1}{q^{r(2n-3r)} |GL(r, q)| |GL(n-2r, q)|}$$

is equal to

$$(6) \quad \frac{\prod_i (1 + u\sqrt{q}/q^i)}{(1 - u^2) \prod_i (1 - u^2/q^i)}.$$

First consider the  $n \rightarrow \infty$  limit of the coefficient of  $u^n$  in (5). This is equal to

$$\begin{aligned} &\lim_{n \rightarrow \infty} \frac{q^{n/2}}{(q^n - 1) \cdots (q - 1)} \sum_{r=0}^{\lfloor n/2 \rfloor} \frac{|GL(n, q)|}{q^{r(2n-3r)} |GL(r, q)| |GL(n-2r, q)|} \\ &= \lim_{n \rightarrow \infty} \frac{q^{n/2}}{(q^n - 1) \cdots (q - 1)} i(n, q) \\ &= \frac{1}{\prod_i (1 - 1/q^i)} \lim_{n \rightarrow \infty} \frac{i(n, q)}{q^{n^2/2}}. \end{aligned}$$

The first equality is from Proposition 3.1.

Now consider (6). Except for poles at  $u = \pm 1$ , it is analytic in a disc of radius greater than 1. Hence Lemma 1.1 gives that for  $n$  even, the  $n \rightarrow \infty$  limit of the coefficient of  $u^n$  in (6) is

$$(7) \quad \frac{1}{2} \left[ \frac{\prod_i (1 + \sqrt{q}/q^i)}{\prod_i (1 - 1/q^i)} + \frac{\prod_i (1 - \sqrt{q}/q^i)}{\prod_i (1 - 1/q^i)} \right].$$

It follows that for  $n$  even,

$$\lim_{n \rightarrow \infty} \frac{i(n, q)}{q^{n^2/2}} = \frac{1}{2} \left[ \prod_{i \geq 1} (1 + \sqrt{q}/q^i) + \prod_{i \geq 1} (1 - \sqrt{q}/q^i) \right].$$

Letting  $Q = 1/q$ , this is equal to

$$\begin{aligned} & \frac{1}{2} \left( (-Q^{1/2}; Q)_\infty + (Q^{1/2}; Q)_\infty \right) \\ &= \frac{1}{2} \left( (-Q^{1/2}; Q^2)_\infty (-Q^{3/2}; Q^2)_\infty + (Q^{1/2}; Q^2)_\infty (Q^{3/2}; Q^2)_\infty \right) \\ &= \frac{1}{2} \frac{1}{(Q^2; Q^2)_\infty} \left( F(Q^{1/2}, Q^2) + F(-Q^{1/2}, Q^2) \right) \\ &= \frac{1}{(Q^2; Q^2)_\infty} F(Q^3, Q^8), \end{aligned}$$

where  $F$  is defined in Proposition 2.6 and where in the last step we have applied Proposition 2.6 with  $X = Q^{1/2}$  and  $R = Q^2$ .

Similarly, if  $n$  is odd, Lemma 1.1 gives that the  $n \rightarrow \infty$  limit of the coefficient of  $u^n$  in (6) is

$$(8) \quad \frac{1}{2} \left[ \frac{\prod_i (1 + \sqrt{q}/q^i)}{\prod_i (1 - 1/q^i)} - \frac{\prod_i (1 - \sqrt{q}/q^i)}{\prod_i (1 - 1/q^i)} \right]$$

It follows that for  $n$  odd,

$$\lim_{n \rightarrow \infty} \frac{i(n, q)}{q^{n^2/2}} = \frac{1}{2} \left[ \prod_{i \geq 1} (1 + \sqrt{q}/q^i) - \prod_{i \geq 1} (1 - \sqrt{q}/q^i) \right].$$

Letting  $Q = 1/q$  and arguing as in the  $n$  even case gives that this is equal to

$$\frac{1}{2} \frac{1}{(Q^2; Q^2)_\infty} \left( F(Q^{1/2}, Q^2) - F(-Q^{1/2}, Q^2) \right) = \frac{1}{\sqrt{q}} \frac{1}{(Q^2; Q^2)_\infty} F(Q^7, Q^8).$$

This proves the theorem.  $\square$

*Remarks:*

- (1) The expression in part 1 of Theorem 3.2 is equal to 1.6793.. when  $q = 2$ , and tends to 1 as  $q \rightarrow \infty$ . The expression in part 2 of Theorem 3.2 is equal to 2.1912.. when  $q = 2$ , and tends to 1 as  $q \rightarrow \infty$ .

- (2) In parts 1 and 2 of Theorem 3.2, one can rewrite the  $(1 - q^{-8i})/(1 - q^{-2i})$  as  $(1 + q^{-4i})(1 + q^{-2i})$ . This makes it clear that the limits in the theorem decrease monotonically to 1 as  $q \rightarrow \infty$ . Our reason for not doing this in the statement of Theorem 3.2 is to emphasize the role in the numerator played by the base 8.

Next we treat odd characteristic. Our main result is the following theorem.

**Theorem 3.3.** (1) *Let  $n$  be even and let  $q$  be odd and fixed. Then*

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{i(n, q)}{q^{n^2/2}} &= \frac{1}{2} \left[ \prod_{i \geq 1} (1 + \sqrt{q}/q^i)^2 + \prod_{i \geq 1} (1 - \sqrt{q}/q^i)^2 \right] \\ &= \prod_{i \geq 1} \frac{(1 + q^{2-4i})^2 (1 - q^{-4i})}{(1 - q^{-i})}. \end{aligned}$$

- (2) *Let  $n$  be odd and let  $q$  be odd and fixed. Then*

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{i(n, q)}{q^{(n^2-1)/2}} &= \frac{\sqrt{q}}{2} \left[ \prod_{i \geq 1} (1 + \sqrt{q}/q^i)^2 - \prod_{i \geq 1} (1 - \sqrt{q}/q^i)^2 \right] \\ &= 2 \prod_{i \geq 1} \frac{(1 + q^{-4i})(1 - q^{-8i})}{(1 - q^{-i})}. \end{aligned}$$

*Proof.* Replacing  $u$  by  $u\sqrt{q}$  in Theorem 2.8 gives the equation

$$(9) \quad \sum_{n \geq 0} u^n q^{n/2} q^{\binom{n}{2}} \sum_{r=0}^n \frac{1}{|GL(r, q)| |GL(n-r, q)|} = \frac{\prod_i (1 + u\sqrt{q}/q^i)^2}{(1 - u^2) \prod_i (1 - u^2/q^i)}.$$

Consider the  $n \rightarrow \infty$  limit of the coefficient of  $u^n$  in the left hand side of (9). This is equal to

$$\begin{aligned} &\lim_{n \rightarrow \infty} \frac{q^{n/2}}{(q^n - 1) \cdots (q - 1)} \sum_{r=0}^n \frac{|GL(n, q)|}{|GL(r, q)| |GL(n-r, q)|} \\ &= \lim_{n \rightarrow \infty} \frac{q^{n/2}}{(q^n - 1) \cdots (q - 1)} i(n, q) \\ &= \frac{1}{\prod_i (1 - 1/q^i)} \lim_{n \rightarrow \infty} \frac{i(n, q)}{q^{n^2/2}}. \end{aligned}$$

The first equality is from Proposition 3.1.

Now consider the right hand side of (9). Except for poles at  $u = \pm 1$ , it is analytic in a disc of radius greater than 1. Hence Lemma 1.1 gives that for  $n$  even, the  $n \rightarrow \infty$  limit of the coefficient of  $u^n$  in the right hand side of (9) is

$$\frac{1}{2} \left[ \frac{\prod_i (1 + \sqrt{q}/q^i)^2}{\prod_i (1 - 1/q^i)} + \frac{\prod_i (1 - \sqrt{q}/q^i)^2}{\prod_i (1 - 1/q^i)} \right].$$



It follows that for  $n$  even,

$$\lim_{n \rightarrow \infty} \frac{i(n, q)}{q^{n^2/2}} = \frac{1}{2} \left[ \prod_{i \geq 1} (1 + \sqrt{q}/q^i)^2 + \prod_{i \geq 1} (1 - \sqrt{q}/q^i)^2 \right].$$

Letting  $Q = 1/q$  and  $F$  be as in Proposition 2.6, this is equal to

$$\frac{1}{2} \frac{1}{(Q; Q)_\infty} \left( F(Q^{1/2}, Q) + F(-Q^{1/2}, Q) \right) = \frac{1}{(Q; Q)_\infty} F(Q^2, Q^4),$$

where we have used Proposition 2.6.

Similarly, if  $n$  is odd, Lemma 1.1 gives that the  $n \rightarrow \infty$  limit of the coefficient of  $u^n$  in the right hand side of (9) is

$$\frac{1}{2} \left[ \frac{\prod_i (1 + \sqrt{q}/q^i)^2}{\prod_i (1 - 1/q^i)} - \frac{\prod_i (1 - \sqrt{q}/q^i)^2}{\prod_i (1 - 1/q^i)} \right].$$

It follows that for  $n$  odd,

$$\lim_{n \rightarrow \infty} \frac{i(n, q)}{q^{n^2/2}} = \frac{1}{2} \left[ \prod_{i \geq 1} (1 + \sqrt{q}/q^i)^2 - \prod_{i \geq 1} (1 - \sqrt{q}/q^i)^2 \right].$$

Letting  $Q = 1/q$ , this is equal to

$$\frac{1}{2} \frac{1}{(Q; Q)_\infty} \left( F(Q^{1/2}, Q) - F(-Q^{1/2}, Q) \right) = \frac{1}{\sqrt{q}} \frac{1}{(Q; Q)_\infty} F(Q^4, Q^4).$$

This proves the theorem.  $\square$

*Remark:* The expression in part 1 of Theorem 3.3 is equal to 2.1825.. when  $q = 3$ , and tends to 1 as  $q \rightarrow \infty$ . The expression in part 2 of Theorem 3.3 is equal to 3.6147.. when  $q = 3$ , and tends to 2 as  $q \rightarrow \infty$ .

#### 4. UNITARY GROUPS

This section studies the asymptotics of the number of involutions in the finite unitary groups  $U(n, q)$ . Throughout we let  $i(n, q)$  denote the number of involutions in  $U(n, q)$ . Recall that in any characteristic

$$(10) \quad |U(n, q)| = q^{n(n-1)/2} \prod_{i=1}^n (q^i - (-1)^i).$$

The following elementary fact was proved in [3].

**Proposition 4.1.** *The number of involutions in  $U(n, q)$  is*

$$i(n, q) = \begin{cases} \sum_{r=0}^{\lfloor n/2 \rfloor} \frac{|U(n, q)|}{q^{r(2n-3r)} |U(r, q)| |U(n-2r, q)|}, & \text{for } q \text{ even,} \\ \sum_{r=0}^n \frac{|U(n, q)|}{|U(r, q)| |U(n-r, q)|}, & \text{for } q \text{ odd.} \end{cases}$$

*Remark:* It is immediate from Propositions 3.1 and 4.1 that the proportion of involutions in  $U(n, q)$  is at most the proportion of involutions in  $GL(n, q)$ , for all values of  $n$  and  $q$ .

To begin we treat the case of even characteristic.

**Theorem 4.2.** (1) *Let  $n$  be even and let  $q$  be even and fixed. Then*

$$\lim_{n \rightarrow \infty} \frac{i(n, q)}{q^{n^2/2}} = \prod_{k \geq 1} \frac{(1 - q^{3-8k})(1 - q^{5-8k})(1 - q^{-8k})}{(1 - q^{-2k})}.$$

(2) *Let  $n$  be odd and let  $q$  be even and fixed. Then*

$$\lim_{n \rightarrow \infty} \frac{i(n, q)}{q^{(n^2-1)/2}} = \prod_{k \geq 1} \frac{(1 - q^{1-8k})(1 - q^{7-8k})(1 - q^{-8k})}{(1 - q^{-2k})}.$$

*Proof.* Since  $|U(n, q)| = (-1)^n |GL(n, -q)|$ , it follows from Proposition 4.1 and Theorem 2.7 that

$$\sum_{n \geq 0} \frac{u^n i(n, q)}{(-1)^{n+\binom{n}{2}} (q^n - (-1)^n) \cdots (q+1)} = \prod_{j \geq 1} \frac{(1 + u/(-q)^j)}{(1 - u^2/(-q)^j)}.$$

Replacing  $u$  by  $u\sqrt{q}$  gives

(11)

$$\sum_{n \geq 0} \frac{u^n i(n, q) q^{n/2}}{(-1)^{n+\binom{n}{2}} (q^n - (-1)^n) \cdots (q+1)} = \prod_{j \geq 1} \frac{(1 + u\sqrt{q}/(-q)^j)}{(1 + u^2) \prod_{j \geq 1} (1 + u^2/(-q)^j)}.$$

Now suppose that  $n = 0 \pmod{4}$ . Then the  $n \rightarrow \infty$  limit of the coefficient of  $u^n$  in the left hand side of (11) is equal to

$$\frac{1}{(1 + 1/q)(1 - 1/q^2) \cdots} \lim_{n \rightarrow \infty} \frac{i(n, q)}{q^{n^2/2}}.$$

Applying Lemma 1.1 gives that the  $n \rightarrow \infty$  limit of the coefficient of  $u^n$  in the right hand side of (11) is equal to

$$\frac{1}{2} \left[ \prod_{j \geq 1} \frac{1 + i\sqrt{q}/(-q)^j}{1 - 1/(-q)^j} + \prod_{j \geq 1} \frac{1 - i\sqrt{q}/(-q)^j}{1 - 1/(-q)^j} \right].$$

It follows from this and Theorem 2.9 that if  $n = 0 \pmod{4}$ , then

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{i(n, q)}{q^{n^2/2}} &= \frac{1}{2} \left[ \prod_{j \geq 1} (1 + i\sqrt{q}/(-q)^j) + \prod_{j \geq 1} (1 - i\sqrt{q}/(-q)^j) \right] \\ &= \prod_{k \geq 1} \frac{(1 - q^{3-8k})(1 - q^{5-8k})(1 - q^{-8k})}{(1 - q^{-2k})}. \end{aligned}$$

A nearly identical argument shows that the same holds when  $n = 2 \pmod{4}$ .

Now suppose that  $n = 1 \pmod{4}$ . Then the  $n \rightarrow \infty$  limit of the coefficient of  $u^n$  in the left hand side of (11) is equal to

$$-\frac{1}{(1 + 1/q)(1 - 1/q^2) \cdots} \lim_{n \rightarrow \infty} \frac{i(n, q)}{q^{n^2/2}}.$$

Applying Lemma 1.1 gives that the  $n \rightarrow \infty$  limit of the coefficient of  $u^n$  in the right hand side of (11) is equal to

$$\frac{1}{2} \left[ \frac{1}{i} \prod_{j \geq 1} \frac{1 + i\sqrt{q}/(-q)^j}{1 - 1/(-q)^j} - \frac{1}{i} \prod_{j \geq 1} \frac{1 - i\sqrt{q}/(-q)^j}{1 - 1/(-q)^j} \right].$$

It follows from this and Theorem 2.10 that if  $n = 1 \bmod 4$ , then

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{i(n, q)}{q^{n^2/2}} &= \frac{i}{2} \left[ \prod_{j \geq 1} (1 + i\sqrt{q}/(-q)^j) - \prod_{j \geq 1} (1 - i\sqrt{q}/(-q)^j) \right] \\ &= \frac{1}{\sqrt{q}} \prod_{k \geq 1} \frac{(1 - q^{1-8k})(1 - q^{7-8k})(1 - q^{-8k})}{(1 - q^{-2k})}. \end{aligned}$$

A nearly identical argument shows that the same holds when  $n = 3 \bmod 4$ .  $\square$

*Remark:* The expression in part 1 of Theorem 4.2 is equal to 1.2255.. when  $q = 2$ , and tends to 1 as  $q \rightarrow \infty$ . The expression in part 2 of Theorem 4.2 is equal to .7162.. when  $q = 2$ , and tends to 1 as  $q \rightarrow \infty$ .

Next we treat the case of odd characteristic.

**Theorem 4.3.** (1) *Let  $n$  be even and let  $q$  be odd and fixed. Then*

$$\lim_{n \rightarrow \infty} \frac{i(n, q)}{q^{n^2/2}} = \prod_{k \geq 1} \frac{(1 + q^{2-4k})^2(1 - q^{-4k})}{(1 - (-1/q)^k)}.$$

(2) *Let  $n$  be odd and let  $q$  be odd and fixed. Then*

$$\lim_{n \rightarrow \infty} \frac{i(n, q)}{q^{(n^2-1)/2}} = 2 \prod_{k \geq 1} \frac{(1 + q^{-4k})^2(1 - q^{-4k})}{(1 - (-1/q)^k)}.$$

*Proof.* Since  $|U(n, q)| = (-1)^n |GL(n, -q)|$ , it follows from Proposition 4.1 and Theorem 2.8 that

$$\sum_{n \geq 0} \frac{u^n i(n, q)}{(-1)^{n+} \binom{n}{2} (q^n - (-1)^n) \cdots (q + 1)} = \prod_{j \geq 1} \frac{(1 + u/(-q)^j)^2}{(1 - u^2/(-q)^j)}.$$

Replacing  $u$  by  $u\sqrt{q}$  gives that

$$\sum_{n \geq 0} \frac{u^n i(n, q) q^{n/2}}{(-1)^{n+} \binom{n}{2} (q^n - (-1)^n) \cdots (q + 1)} = \prod_{j \geq 1} \frac{(1 + u\sqrt{q}/(-q)^j)^2}{(1 + u^2) \prod_{j \geq 1} (1 + u^2/(-q)^j)}.$$

Now if  $n$  is even, arguing as in Theorem 4.2 gives that

$$\lim_{n \rightarrow \infty} \frac{i(n, q)}{q^{n^2/2}} = \frac{1}{2} \left[ \prod_{j \geq 1} (1 + i\sqrt{q}/(-q)^j)^2 + \prod_{j \geq 1} (1 - i\sqrt{q}/(-q)^j)^2 \right].$$

The result now follows from Theorem 2.11.

If  $n$  is odd, arguing as in Theorem 4.2 gives that

$$\lim_{n \rightarrow \infty} \frac{i(n, q)}{q^{n^2/2}} = \frac{i}{2} \left[ \prod_{j \geq 1} (1 + i\sqrt{q}/(-q)^j)^2 - \prod_{j \geq 1} (1 - i\sqrt{q}/(-q)^j)^2 \right].$$

The result now follows from Theorem 2.12.  $\square$

*Remark:* The expression in part 1 of Theorem 4.3 is equal to 1.0040.. when  $q = 3$ , and tends to 1 as  $q \rightarrow \infty$ . The expression in part 2 of Theorem 4.3 is equal to 1.6627.. when  $q = 3$ , and tends to 2 as  $q \rightarrow \infty$ .

## 5. SYMPLECTIC GROUPS

This section studies the asymptotics of the number of involutions in the finite symplectic groups. We begin with the case of odd characteristic.

**Lemma 5.1.** *Suppose that the characteristic is odd. Then the number of involutions in  $Sp(2n, q)$  is equal to*

$$\sum_{r=0}^n \frac{|Sp(2n, q)|}{|Sp(2r, q)||Sp(2n-2r, q)|}.$$

*Proof.* Let  $g \in Sp(2n, q)$  be an involution. Let  $V$  denote the natural  $2n$ -dimensional module. Then  $V = V_{-1} \perp V_1$  where  $V_a$  is the eigenspace of  $g$  with eigenvalue  $a$ . Note that each  $V_1$  is a nondegenerate space of even dimension. Set  $2r = \dim V_1$ . Since any two nondegenerate spaces of the same dimension are in the same  $Sp(2n, q)$  orbit, we see the conjugacy classes of involutions are determined by  $r$ . Moreover, the centralizer of  $g$  is obviously isomorphic to  $Sp(2r, q) \times Sp(2n-2r, q)$  and so the size of the conjugacy class of  $g$  is

$$\frac{|Sp(2n, q)|}{|Sp(2r, q)||Sp(2n-2r, q)|}.$$

Since  $r$  can take on any value between 0 and  $n$ , this proves the theorem.  $\square$

The following theorem is our main result.

**Theorem 5.2.** *Let  $i(2n, q)$  be the number of involutions in  $Sp(2n, q)$ .*

(1) *Let  $n$  be even and  $q$  be odd and fixed. Then*

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{i(2n, q)}{q^{n^2}} &= \frac{1}{2} \left[ \prod_{i \geq 1} (1 + 1/q^{2i-1})^2 + \prod_{i \geq 1} (1 - 1/q^{2i-1})^2 \right] \\ &= \prod_{i \geq 1} \frac{(1 + q^{4-8i})^2 (1 - q^{-8i})}{(1 - q^{-2i})}. \end{aligned}$$

(2) Let  $n$  be odd and  $q$  be odd and fixed. Then

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{i(2n, q)}{q^{n^2-1}} &= \frac{q}{2} \left[ \prod_{i \geq 1} (1 + 1/q^{2i-1})^2 - \prod_{i \geq 1} (1 - 1/q^{2i-1})^2 \right] \\ &= 2 \prod_{i \geq 1} \frac{(1 + q^{-8i})(1 - q^{-16i})}{(1 - q^{-2i})}. \end{aligned}$$

*Proof.* Replacing  $u$  by  $uq$  in Theorem 2.13 gives

(12)

$$\sum_{n \geq 0} u^n q^{n^2+n} \sum_{r=0}^n \frac{1}{|Sp(2r, q)| |Sp(2n-2r, q)|} = \frac{\prod_i (1 + u/q^{2i-1})^2}{(1 - u^2) \prod_i (1 - u^2/q^{2i})}.$$

Consider the  $n \rightarrow \infty$  limit of the coefficient of  $u^n$  in the left hand side of (12). This is equal to

$$\begin{aligned} &\lim_{n \rightarrow \infty} \frac{1}{q^{n^2} (1 - 1/q^2) \cdots (1 - 1/q^{2n})} \sum_{r=0}^n \frac{|Sp(2n, q)|}{|Sp(2r, q)| |Sp(2n-2r, q)|} \\ &= \lim_{n \rightarrow \infty} \frac{1}{q^{n^2} (1 - 1/q^2) \cdots (1 - 1/q^{2n})} i(2n, q) \\ &= \frac{1}{\prod_i (1 - 1/q^{2i})} \lim_{n \rightarrow \infty} \frac{i(2n, q)}{q^{n^2}}. \end{aligned}$$

The first equality was Lemma 5.1.

Now consider the right hand side of (12). Except for poles at  $u = \pm 1$ , it is analytic in a disc of radius greater than 1. Hence Lemma 1.1 gives that for  $n$  even, the  $n \rightarrow \infty$  limit of the coefficient of  $u^n$  in the right hand side of (12) is

$$\frac{1}{2} \left[ \frac{\prod_i (1 + 1/q^{2i-1})^2}{\prod_i (1 - 1/q^{2i})} + \frac{\prod_i (1 - 1/q^{2i-1})^2}{\prod_i (1 - 1/q^{2i})} \right].$$

It follows that for  $n$  even,

$$\lim_{n \rightarrow \infty} \frac{i(2n, q)}{q^{n^2}} = \frac{1}{2} \left[ \prod_{i \geq 1} (1 + 1/q^{2i-1})^2 + \prod_{i \geq 1} (1 - 1/q^{2i-1})^2 \right].$$

Letting  $Q = 1/q$  and using Proposition 2.6 gives that this is equal to

$$\frac{1}{2} \frac{1}{(Q^2; Q^2)_\infty} (F(Q, Q^2) + F(-Q, Q^2)) = \frac{1}{(Q^2; Q^2)_\infty} F(Q^4, Q^8).$$

Similarly, if  $n$  is odd, Lemma 1.1 gives that the  $n \rightarrow \infty$  limit of the coefficient of  $u^n$  in the right hand side of (12) is

$$\frac{1}{2} \left[ \frac{\prod_i (1 + 1/q^{2i-1})^2}{\prod_i (1 - 1/q^{2i})} - \frac{\prod_i (1 - 1/q^{2i-1})^2}{\prod_i (1 - 1/q^{2i})} \right].$$

It follows that for  $n$  odd,

$$\lim_{n \rightarrow \infty} \frac{i(2n, q)}{q^{n^2}} = \frac{1}{2} \left[ \prod_{i \geq 1} (1 + 1/q^{2i-1})^2 - \prod_{i \geq 1} (1 - 1/q^{2i-1})^2 \right].$$

Letting  $Q = 1/q$  and using Proposition 2.6 gives that this is equal to

$$\frac{1}{2} \frac{1}{(Q^2; Q^2)_\infty} (F(Q, Q^2) - F(-Q, Q^2)) = \frac{1}{(Q^2; Q^2)_\infty} Q F(Q^8, Q^8).$$

This proves the theorem.  $\square$

*Remark:* The expression in part 1 of Theorem 5.2 is equal to 1.1689.. when  $q = 3$ , and tends to 1 as  $q \rightarrow \infty$ . The expression in part 2 of Theorem 5.2 is equal to 2.2819.. when  $q = 3$ , and tends to 2 as  $q \rightarrow \infty$ .

Next we consider the case that  $q$  is even.

To begin we use elementary means to derive a formula for the number of involutions in  $Sp(2n, q)$  when  $q$  is even. For related results, see [2] or [4].

**Theorem 5.3.** *When  $q$  is even, the number of involutions in  $Sp(2n, q)$  is equal to*

$$\sum_{\substack{r=0 \\ r \text{ even}}}^n \frac{|Sp(2n, q)|}{A_r} + \sum_{\substack{r=1 \\ r \text{ even}}}^n \frac{|Sp(2n, q)|}{B_r} + \sum_{\substack{r=1 \\ r \text{ odd}}}^n \frac{|Sp(2n, q)|}{C_r}$$

where

$$\begin{aligned} A_r &= q^{r(r+1)/2 + r(2n-2r)} |Sp(r, q)| |Sp(2n-2r, q)|, \\ B_r &= q^{r(r+1)/2 + r(2n-2r)} q^{r-1} |Sp(r-2, q)| |Sp(2n-2r, q)|, \\ C_r &= q^{r(r+1)/2 + r(2n-2r)} |Sp(r-1, q)| |Sp(2n-2r, q)|. \end{aligned}$$

The following lemma will be helpful for proving Theorem 5.3.

**Lemma 5.4.** *Suppose  $q$  is even, and let  $g \in Sp(2n, q)$  be an involution. Let  $V$  be the natural module of dimension  $2n$  for  $Sp(2n, q)$ . Then*

- (1)  $W = (g - 1)V$  is totally singular of dimension  $r$ , where  $r \leq n$  is the rank of  $g - 1$ .
- (2)  $W^\perp = V^g$  is the fixed space of  $g$  on  $V$ .

*Proof.* If  $U$  is a nontrivial nondegenerate subspace of  $V^g$ , then clearly,  $V = U \oplus U^\perp$  is a  $g$ -stable decomposition whence the result follows by induction.

So we may assume that  $V^g$  is totally singular. Since  $\dim V^g \geq n$ , it follows that  $V^g$  is  $n$ -dimensional and is a maximal isotropic space. Since  $g^2 = 1$ ,  $W \leq V^g$  and since  $\dim W + \dim V^g = 2n$ , we see in this case that  $r = n$  and  $V^g = W^\perp$  and the result holds.  $\square$

Now we prove Theorem 5.3.

*Proof.* (Of Theorem 5.3) Let  $g \in G$  be an involution. With respect to the flag  $0 < (g-1)V < V^g < V$ ,  $g$  can be written as:

$$\begin{pmatrix} I & 0 & h \\ 0 & I & 0 \\ 0 & 0 & I \end{pmatrix}$$

Since  $g \in G$ , it follows that  $h$  is a symmetric matrix of rank  $r$ . Let  $P$  be the parabolic subgroup stabilizing the flag. Then  $P$  acts on the set of all such elements with any symmetric element in the upper corner by congruence (via  $GL(r, q)$ ).

We use the fact that two symmetric  $m \times m$  matrices over a perfect field of characteristic 2 are congruent if and only if they have the same rank and are both skew or are both nonskew (in particular if the rank is odd, then they are all congruent).

Thus, we see that the conjugacy classes of involutions in  $G$  are determined by the rank  $r$  and if  $r > 0$  is even on whether  $h$  is skew or not. Clearly, two involutions written as above are conjugate in  $G$  if and only if they are conjugate in  $P$  if and only if the right hand corner terms are congruent. In particular, there are  $n+1+n/2$  classes if  $n$  is even and  $n+1+(n-1)/2$  classes if  $n$  is odd.

Now we can write down the centralizers of such elements. Clearly any element of  $C_G(g)$  preserves the flag and so  $C_G(g)$  is contained in  $P$ .

Note that  $P = LQ$  where  $Q$  is the unipotent radical with

$$|Q| = q^{r(r+1)/2 + r(2n-2r)}.$$

Clearly  $Q$  centralizes  $g$ . Note that  $L = GL(r, q) \times Sp(2n-2r, q)$  and that  $Sp(2n-2r, q)$  also centralizes  $g$ . So we just need to compute the centralizer of  $g$  in  $K := GL(r, q)$ . Now  $A \in K$  acts on  $g$  by sending  $h$  to  $AhA^\top$ . Thus,  $C_K(g) \cong Sp(r, q)$  if  $r$  is even and  $h$  is an alternating form.

If  $h$  is not alternating, by the remarks above, we can take  $h = I$  and so  $C_K(g) = \{A \in K \mid AA^\top = I\}$ . Of course, if  $q$  were odd, this would just be an orthogonal group. However, with  $q$  even, this is not the case. We now compute the order of  $C_K(g)$ .

Let  $U$  be an  $r$ -dimensional space with a nondegenerate symmetric bilinear pairing  $(,)$  on  $U$  that is not alternating (so  $(u, u) = 1$  for some  $u \in U$ ). Let  $U_1$  be the set of all  $u$  with  $(u, u) = 0$ . Since we are in a field of characteristic 2, this is a hyperplane in  $U$ . Note that the form restricted to  $U_1$  is alternating. Set  $U_0 = U_1^\perp$ . Note that  $U_0$  is 1-dimensional (because our form is nondegenerate).

If  $U_0 \cap U_1 = 0$ , then  $r$  is odd and  $L$  preserves this decomposition whence  $C_K(g) \cong Sp(r-1, q)$  (the action is determined precisely by the action on  $U_1$  since it must be trivial on  $U_0$  and preserve the splitting).

If  $U_0 < U_1$ , then  $U_1/U_0$  is a nonsingular space of dimension  $r-2$  with the corresponding alternating form and so  $r$  is even.

In this case any element of  $C_K(g)$  is trivial on  $U_0$ . Let  $v \in U$  be a vector with  $v$  outside of  $U_0$  with  $(v, v) = 1$ . Then there exists  $x \in C_K(g)$  with  $xv = v + u$  for any  $u \in U_1$ . Moreover,  $C_K(g)$  induces  $Sp(r-2, q)$  on  $U_0/U_1$  and it is an easy exercise to see that

$$|C_K(g)| = |Sp(r-2, q)|q^{r-1}.$$

Summarizing, we can write down the orders of centralizers for each class representative:

For each even  $r$  with  $0 \leq r \leq n$ , we have a class  $C(r)$  with the centralizer having order

$$A_r = q^{r(r+1)/2+r(2n-2r)} |Sp(r, q)| |Sp(2n-2r, q)|.$$

For each  $r$  with  $1 \leq r \leq n$ , we have a class  $D(r)$  with centralizer having order for  $r$  even:

$$B_r = q^{r(r+1)/2+r(2n-2r)} q^{r-1} |Sp(r-2, q)| |Sp(2n-2r, q)|.$$

and for  $r$  odd:

$$C_r = q^{r(r+1)/2+r(2n-2r)} |Sp(r-1, q)| |Sp(2n-2r, q)|.$$

Adding these contributions completes the proof.  $\square$

This leads to the following result.

**Theorem 5.5.** *Let  $i(2n, q)$  be the number of involutions in  $Sp(2n, q)$ . Let  $q$  be even and fixed. Then*

$$\lim_{n \rightarrow \infty} \frac{i(2n, q)}{q^{n^2+n}} = \prod_{i \geq 1} (1 + 1/q^{2i}).$$

*Proof.* Combining Theorem 5.3 and Theorem 2.14 gives that

$$(13) \quad \sum_{n \geq 0} u^n q^{n^2} \frac{i(2n, q)}{|Sp(2n, q)|} = \frac{1}{1-u} \frac{\prod_{i \geq 1} (1 + u/q^{2i})}{\prod_{i \geq 1} (1 - u^2/q^{2i})}.$$

Consider the  $n \rightarrow \infty$  limit of the coefficient of  $u^n$  in the left hand side of (13). This is equal to

$$\begin{aligned} & \lim_{n \rightarrow \infty} \frac{i(2n, q)}{q^{n^2+n} \prod_{i=1}^n (1 - 1/q^{2i})} \\ &= \frac{1}{\prod_{i \geq 1} (1 - 1/q^{2i})} \lim_{n \rightarrow \infty} \frac{i(2n, q)}{q^{n^2+n}}. \end{aligned}$$

Now consider the right hand side of (13). Except for a pole at  $u = 1$ , it is analytic in a disc of radius greater than 1. Hence Lemma 1.1 gives that the  $n \rightarrow \infty$  of the coefficient of  $u^n$  in the right hand side of (13) is

$$\frac{\prod_{i \geq 1} (1 + 1/q^{2i})}{\prod_{i \geq 1} (1 - 1/q^{2i})}.$$

The theorem follows.  $\square$



*Remark:* The expression in Theorem 5.5 is equal to 1.3559.. when  $q = 2$ , and tends to 1 as  $q \rightarrow \infty$ .

## 6. ORTHOGONAL GROUPS

This section studies the asymptotics of the number of involutions in orthogonal groups. We assume first that the characteristic is odd.

Lemma 6.1 gives an exact expression for the number of involutions. We note that the two terms in part 2 of Lemma 6.1 are equal.

**Lemma 6.1.** *Suppose that the characteristic is odd.*

(1) *The number of involutions in  $O^+(2n, q)$  is equal to*

$$\sum_{r=0}^{2n} \frac{|O^+(2n, q)|}{|O^+(r, q)||O^+(2n-r, q)|} + \sum_{r=1}^{2n-1} \frac{|O^+(2n, q)|}{|O^-(r, q)||O^-(2n-r, q)|}.$$

(2) *The number of involutions in  $O^-(2n, q)$  is equal to*

$$\sum_{r=0}^{2n-1} \frac{|O^-(2n, q)|}{|O^+(r, q)||O^-(2n-r, q)|} + \sum_{r=1}^{2n} \frac{|O^-(2n, q)|}{|O^-(r, q)||O^+(2n-r, q)|}.$$

(3) *The number of involutions in  $O^+(2n+1, q)$  (or in  $O^-(2n+1, q)$ ) is equal to*

$$\sum_{r=0}^{2n+1} \frac{|O^+(2n+1, q)|}{|O^+(r, q)||O^+(2n+1-r, q)|} + \sum_{r=1}^{2n} \frac{|O^+(2n+1, q)|}{|O^-(r, q)||O^-(2n+1-r, q)|}.$$

*Proof.* Let  $g \in O^\pm(n, q)$  be an involution and let  $V$  denote the natural orthogonal module. Then  $V = V_1 \perp V_{-1}$  where  $V_1$  is the fixed space of  $g$  and  $V_{-1}$  is the  $-1$  eigenspace of  $g$ . In particular, these eigenspaces are nondegenerate. Let  $r = \dim V_1$ .

The conjugacy class of  $g$  is determined by the orbit of  $V_1$  under the orthogonal group. Given a fixed  $r$  with  $0 < r < n$ , there will be two orbits depending upon the type of  $V_1$  (note that the type of  $V$  and  $V_1$  determines the type of  $V_{-1}$ ). If  $r = 0$  or  $n$ , then  $g$  is a scalar.

Clearly the centralizer of  $g$  is  $O(V_1) \times O(V_{-1})$  and so the size of the conjugacy class of  $g$  is

$$\frac{|O^\pm(n, q)|}{|O(V_1)||O(V_{-1})|},$$

whence the result. □

This leads to the following result.

**Theorem 6.2.** *Let  $i^\pm(2n, q)$  denote the number of involutions in  $O^\pm(2n, q)$ . Let  $q$  be odd and fixed. Then*

$$\lim_{n \rightarrow \infty} \frac{i^\pm(2n, q)}{q^{n^2}} = \prod_{i \geq 1} (1 + 1/q^{2i-1})^2.$$

*Proof.* We prove the assertion for  $i^+(2n, q)$  as the proof for  $i^-(2n, q)$  is almost identical (using part 2 of Lemma 6.1 instead of part 1 of Lemma 6.1, and Theorem 2.16 instead of Theorem 2.15).

Replacing  $u$  by  $u/q$  in Theorem 2.15, and applying part 1 of Lemma 6.1 gives that

$$(14) \quad \frac{1}{2(1-u)} \frac{\prod_i (1 + u/q^{2i-1})^2}{\prod_i (1 - u^2/q^{2i})} + \frac{1}{2} \frac{\prod_i (1 + u/q^{2i})^2}{\prod_i (1 - u^2/q^{2i})}$$

is equal to

$$(15) \quad \sum_{n \geq 0} \frac{u^n i^+(2n, q)}{2(1 - 1/q^n)(1 - 1/q^2) \cdots (1 - 1/q^{2(n-1)})q^{n^2}}.$$

Taking the  $n \rightarrow \infty$  limit of the coefficient of  $u^n$  in (15) gives

$$\frac{1}{2 \prod_i (1 - 1/q^{2i})} \lim_{n \rightarrow \infty} \frac{i^+(2n, q)}{q^{n^2}}.$$

Consider the  $n \rightarrow \infty$  limit of the coefficient of  $u^n$  in the first infinite product in (14); by Lemma 1.1, it is equal to

$$\frac{1}{2} \frac{\prod_i (1 + 1/q^{2i-1})^2}{\prod_i (1 - 1/q^{2i})}.$$

Since the second term of (14) is analytic in a disc of radius bigger than 1, it follows that the  $n \rightarrow \infty$  limit of the coefficient of  $u^n$  in the second infinite product of (14) is equal to 0.

Summarizing, we have shown that

$$\frac{1}{2 \prod_i (1 - 1/q^{2i})} \lim_{n \rightarrow \infty} \frac{i^+(2n, q)}{q^{n^2}} = \frac{1}{2} \frac{\prod_i (1 + 1/q^{2i-1})^2}{\prod_i (1 - 1/q^{2i})},$$

which implies the theorem.  $\square$

*Remark:* The expression in Theorem 6.2 is equal to 1.9296.. when  $q = 3$ , and tends to 1 as  $q \rightarrow \infty$ .

We next treat the case of odd dimensional orthogonal groups in odd characteristic.

**Theorem 6.3.** *Let  $i(2n+1, q)$  be the number of involutions in  $O(2n+1, q)$ . Let  $q$  be odd and fixed. Then*

$$\lim_{n \rightarrow \infty} \frac{i(2n+1, q)}{q^{n^2+n}} = 2 \prod_{i \geq 1} (1 + 1/q^{2i})^2.$$

*Proof.* It follows from Theorem 2.17 and part 3 of Lemma 6.1 that

$$(16) \quad \sum_{n \geq 0} u^n q^{n^2} \frac{i(2n+1, q)}{|O(2n+1, q)|} = \frac{1}{1-u} \frac{\prod_i (1 + u/q^{2i})^2}{\prod_i (1 - u^2/q^{2i})}.$$

The  $n \rightarrow \infty$  limit of the coefficient of  $u^n$  on the left hand side of (16) is equal to

$$\frac{1}{2 \prod_i (1 - 1/q^{2i})} \lim_{n \rightarrow \infty} \frac{i(2n+1, q)}{q^{n^2+n}}.$$

By Lemma 1.1, the  $n \rightarrow \infty$  limit of the coefficient of  $u^n$  on the right hand side of (16) is equal to

$$\frac{\prod_i (1 + 1/q^{2i})^2}{\prod_i (1 - 1/q^{2i})}.$$

Comparing these two expressions proves the theorem.  $\square$

*Remark:* The expression in Theorem 6.3 is equal to 2.5382.. when  $q = 3$ , and tends to 2 as  $q \rightarrow \infty$ .

Next we give results for even characteristic orthogonal groups. Note that it is not necessary to treat odd dimensional orthogonal groups in even characteristic, as these are isomorphic to symplectic groups.

To begin, we derive a formula for the number of involutions in even characteristic orthogonal groups. Let  $G = O^\epsilon(2n, q)$  with  $q$  a power of 2. Let  $\nu$  denote the quadratic form preserved by  $G$  on the natural module  $V$  of dimension  $2n$ . Recall that  $\nu$  defines by a nondegenerate  $G$ -invariant alternating form on  $V$  defined by

$$(v, w) := \nu(v + w) + \nu(v) + \nu(w).$$

If  $g \in G$  is an involution, then  $g \in X = Sp(2n, q)$  with respect to the alternating form defined above.

So by Lemma 5.4,  $W := (g - 1)V$  is totally singular with respect to the alternating form of rank  $r$ .

We next note:

**Lemma 6.4.** *If  $x, g \in G$  are involutions and are conjugate in  $X$ , then they are conjugate in  $G$ .*

*Proof.* If  $2n = 2$  or  $4$ , this is clear. So assume that  $2n \geq 6$ .

If  $g$  is a transvection in  $X$ , then we see that  $g$  is trivial on nondegenerate 2-spaces of either type (and so is  $x$ ), whence the result follows by induction.

Suppose next that  $g$  corresponds to a symmetric element in  $X$  of rank at least 2. Then  $g$  leaves invariant a nondegenerate 4-space where it has 2 Jordan blocks of size 2 with each nondegenerate. Working in  $Sp(4, q)$ , we see that  $g$  preserves nondegenerate 2-spaces of either type (where it acts nontrivially) and so the result follows by induction.

Suppose that  $g$  corresponds to a skew element in  $X$ . We see from the section on even characteristic symplectic groups that  $V$  is an orthogonal direct sum of 4-dimensional subspaces and one space where  $g$  acts trivially. If the last space is actually there, we see by reducing to the case that  $2n = 6$ , that  $g$  acts trivially on 2-dimensional invariant subspaces of both types, whence the result follows by induction. So the remaining case is that all Jordan blocks have size 2. It follows that on each 4-dimensional block above, the

type must be  $+$  (such elements do not live in  $O^-(4, q)$ , which is isomorphic to  $SL(2, q^2).2$ , the semidirect product of  $SL(2, q^2)$  with a group of order 2 whose generator induces the field automorphism on  $SL(2, q^2)$  given by the  $q$ th power map on the field of size  $q^2$ ), whence the type of  $G$  must be  $+$  as well and the result is clear in this case.  $\square$

It also follows from the argument above that each class in  $X$  occurs in  $G$  unless  $g$  corresponds to an alternating element in  $X$  of rank  $n$  (and so  $n$  is even). In the latter case,  $g$  can only be in  $O^+(2n, q)$ . In the proof of Theorem 5.3, the conjugacy classes of involutions in  $Sp$  were called  $C(r)$  and  $D(r)$ . Let  $C^\epsilon(r)$  and  $D^\epsilon(r)$  denote the intersections with  $G$  (of type  $\epsilon$ ). By the previous lemma, this is either empty or a conjugacy class in  $G$ .

Now we have to compute centralizers.

As noted if  $g$  is in  $C(r)$  with  $r$  even, then  $g$  is conjugate to an element of  $G$  unless  $r = n$  and  $\epsilon = -$ .

Then  $g$  may be written as:

$$\begin{pmatrix} I & 0 & h \\ 0 & I & 0 \\ 0 & 0 & I \end{pmatrix},$$

where  $h$  is skew of rank  $r$ .

We see that  $g \in G_0 := SO^\epsilon(2n, q)$  and

$$|C_G(g)| = |Sp(r, q)| |O^\epsilon(2n - 2r, q)| q^{r(2n-2r)} q^{r(r-1)/2}.$$

Note that if  $r = n$ , then the  $O$  part of the centralizer is not there and  $\epsilon = +$ . Note also that if  $r < n$ , the  $G$  and  $G_0$  classes are the same (because  $g$  commutes with a transvection in  $G$ ) while if  $r = n$ , there is a single  $G$ -class that splits into 2  $G_0$  classes (corresponding to the classes of maximal totally isotropic subspaces).

We can compare  $|C^\epsilon(r)|$  and  $|C(r)|$ . We have

$$|C^\epsilon(r)| = [G : C_G(g)] = \frac{|G||C_X(g)|}{|X||C_G(g)|} |C(r)| = \frac{q^{n-r} + \epsilon 1}{q^n + \epsilon 1} |C(r)|.$$

The above formula again shows that  $|C^-(n)| = 0$ .

Next we consider the classes  $D(r)$  with  $1 \leq r \leq n$ . Note that for any such element we can write  $V$  as an orthogonal sum of nondegenerate 2-dimensional invariant spaces. This implies that the  $G$ -classes and  $G_0$  classes coincide (since any such element commutes with a transvection which is in  $G$  but not in  $G_0$ ).

Consider  $X$  acting on the orthogonal module of dimension  $2n + 1$  (this is an indecomposable  $X$ -module with a 1-dimensional socle). The stabilizers of the complements to the 1-dimensional socle are precisely the orthogonal groups contained in  $X$ . Of course, the number of complements is  $q^{2n}$ . If  $g \in D(r)$ , then the number of  $g$ -invariant complements is  $q^{2n-r}$ . Thus,  $g$  lives in a total of  $q^{2n-r}$  different orthogonal subgroups of  $X$ .

**Lemma 6.5.** *Suppose that  $g \in D(r) \subset X$ . Then  $g$  is in  $q^{2n-r}/2$  orthogonal subgroups of  $X$  of each type.*

*Proof.* We can decompose  $V = V_0 \perp V_1 \perp \dots \perp V_r$  where each  $V_i, i > 0$  is a nondegenerate 2-dimensional space on which  $g$  acts nontrivially and  $g$  acts trivially on  $V_0$ . Any quadratic form giving rise to the given alternating form is determined by its restrictions to each  $V_i$ . Clearly, there are the same number of quadratic forms of each type.  $\square$

Now we can compute  $|D^\epsilon(r)|$ . Let  $g \in D^\epsilon(r)$ .

Let  $\Omega$  be the set of orthogonal subgroups of  $X$  of type  $\epsilon$ . Since any two orthogonal subgroups of the same type are conjugate in  $X$  and their own normalizers (indeed, they are almost always maximal), we see that

$$|\Omega| = [X : O^\epsilon(2n, q)] = q^n(q^n + \epsilon 1)/2.$$

Let  $\Omega(g)$  denote those elements of  $\Omega$  containing  $g$  (so this is the fixed point set of  $g$  acting on  $\Omega$ ). By the previous lemma  $|\Omega(g)| = q^{2n-r}/2$ . An elementary formula (essentially coming from Burnside's Lemma) shows that

$$|\Omega(g)||D(r)| = |\Omega||D^\epsilon(r)|.$$

Thus,

$$|D^\epsilon(r)| = \frac{(1/2)q^{2n-r}}{|\Omega|} |D(r)| = \frac{q^{2n-r}}{q^n(q^n + \epsilon 1)} |D(r)|,$$

and so

$$|D^\epsilon(r)| = \frac{q^{n-r}}{q^n + \epsilon 1} |D(r)|.$$

Of course  $|D(r)|$  was computed in the proof of Theorem 5.3.

Summarizing, we have proved the following theorem.

**Theorem 6.6.** *Let  $q$  be even.*

(1) *The number of involutions in  $O^+(2n, q)$  is equal to*

$$\sum_{\substack{r=0 \\ r \text{ even}}}^n \frac{|O^+(2n, q)|}{A_r} + \sum_{\substack{r=1 \\ r \text{ even}}}^n \frac{|O^+(2n, q)|}{B_r} + \sum_{\substack{r=1 \\ r \text{ odd}}}^n \frac{|O^+(2n, q)|}{C_r}$$

where

$$A_r = q^{r(r-1)/2 + r(2n-2r)} |Sp(r, q)| |O^+(2n-2r, q)|$$

$$B_r = 2q^{r(r+1)/2 + (r-1)(2n-2r)-1} |Sp(r-2, q)| |Sp(2n-2r, q)|$$

$$C_r = 2q^{r(r-1)/2 + (r-1)(2n-2r)} |Sp(r-1, q)| |Sp(2n-2r, q)|.$$

(2) The number of involutions in  $O^-(2n, q)$  is equal to

$$\sum_{\substack{r=0 \\ r \text{ even}}}^{n-1} \frac{|O^-(2n, q)|}{A_r} + \sum_{\substack{r=1 \\ r \text{ even}}}^n \frac{|O^-(2n, q)|}{B_r} + \sum_{\substack{r=1 \\ r \text{ odd}}}^n \frac{|O^-(2n, q)|}{C_r}$$

where

$$A_r = q^{r(r-1)/2 + r(2n-2r)} |Sp(r, q)| |O^-(2n-2r, q)|$$

$$B_r = 2q^{r(r+1)/2 + (r-1)(2n-2r)-1} |Sp(r-2, q)| |Sp(2n-2r, q)|$$

$$C_r = 2q^{r(r-1)/2 + (r-1)(2n-2r)} |Sp(r-1, q)| |Sp(2n-2r, q)|.$$

Note that in the  $A_r$  sum in part 2,  $r$  only ranges from 0 to  $n-1$ , and that the values of  $B_r$  and  $C_r$  are the same in parts 1 and 2 of the theorem.

This leads to the following result.

**Theorem 6.7.** Let  $i^\pm(2n, q)$  denote the number of involutions in  $O^\pm(2n, q)$ . Let  $q$  be even and fixed. Then

$$\lim_{n \rightarrow \infty} \frac{i^\pm(2n, q)}{q^{n^2}} = \prod_{i \geq 1} (1 + 1/q^{2i-1}).$$

*Proof.* We prove the assertion for  $i^+(2n, q)$  as the proof for  $i^-(2n, q)$  is almost identical (using part 2 of Theorem 6.6 instead of part 1 of Theorem 6.6, and Theorem 2.19 instead of Theorem 2.18).

Replacing  $u$  by  $u/q$  in Theorem 2.18 and applying Theorem 6.6 gives that

$$(17) \quad \frac{1}{2(1-u)} \frac{\prod_i (1 + u/q^{2i-1})}{\prod_i (1 - u^2/q^{2i})} + \frac{1}{2} \frac{\prod_i (1 + u/q^{2i})}{\prod_i (1 - u^2/q^{2i})}$$

is equal to

$$(18) \quad \sum_{n \geq 0} \frac{u^n i^+(2n, q)}{2(1 - 1/q^n)(1 - 1/q^2) \cdots (1 - 1/q^{2(n-1)}) q^{n^2}}.$$

Taking the  $n \rightarrow \infty$  limit of the coefficient of  $u^n$  in (18) gives

$$\frac{1}{2 \prod_i (1 - 1/q^{2i})} \lim_{n \rightarrow \infty} \frac{i^+(2n, q)}{q^{n^2}}.$$

Consider the  $n \rightarrow \infty$  limit of the coefficient of  $u^n$  in the first infinite product in (17). By Lemma 1.1, it is equal to

$$\frac{1}{2} \frac{\prod_i (1 + 1/q^{2i-1})}{\prod_i (1 - 1/q^{2i})}.$$

Since the second term of (17) is analytic in a disc of radius bigger than 1, it follows that the  $n \rightarrow \infty$  limit of the coefficient of  $u^n$  in the second infinite product of (17) is equal to 0.

Summarizing, we have shown that

$$\frac{1}{2 \prod_i (1 - 1/q^{2i})} \lim_{n \rightarrow \infty} \frac{i^+(2n, q)}{q^{n^2}} = \frac{1}{2} \frac{\prod_i (1 + 1/q^{2i-1})}{\prod_i (1 - 1/q^{2i})},$$

which implies the theorem.  $\square$

*Remark:* The expression in Theorem 6.7 is equal to 1.7583.. when  $q = 2$ , and tends to 1 as  $q \rightarrow \infty$ .

## 7. ACKNOWLEDGEMENTS

Guralnick was partially supported by NSF grant DMS-1302886. Stanton was partially supported by NSF grant DMS-1148634. The authors are very grateful to Geoff Robinson for helpful correspondence.

## REFERENCES

- [1] Andrews, G., The theory of partitions, Encyclopedia of Mathematics and its Applications, Vol. 2. Addison-Wesley Publishing Co., Reading, Mass.-London-Amsterdam, 1976.
- [2] Aschbacher, M. and Seitz, G., Involutions in Chevalley groups over fields of even order, *Nagoya Math. J.* **63** (1976), 1-91.
- [3] Fulman, J. and Vinroot, R., Generating functions for real character degree sums of finite general linear and unitary groups, *J. Algebr. Comb.* **40** (2014), 387-416.
- [4] Liebeck, M. and Seitz, G., Unipotent and nilpotent classes in simple algebraic groups and Lie algebras, Mathematical Surveys and Monographs, 180. American Math Society, Providence, RI, 2012.
- [5] Morrison, K., Integer sequences and matrices over finite fields, *J. Integer Seq.* **9** (2006), Article 06.2.1, 28 pp.
- [6] Odlyzko, A., Asymptotic enumeration methods, Chapter 22 in Handbook of Combinatorics, Volume 2. MIT Press and Elsevier, 1995.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF SOUTHERN CALIFORNIA, LOS ANGELES, CA 90089-2532

*E-mail address:* `fulman@usc.edu`

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF SOUTHERN CALIFORNIA, LOS ANGELES, CA 90089-2532

*E-mail address:* `guralnic@usc.edu`

SCHOOL OF MATHEMATICS, UNIVERSITY OF MINNESOTA, MINNEAPOLIS, MN 55455

*E-mail address:* `stanton@math.umn.edu`